

# Nuclei of Normal Rational Curves

Johannes Gmainer\*

Hans Havlicek

Abteilung für Lineare Algebra und Geometrie,  
Technische Universität,  
Wiedner Hauptstraße 8–10,  
A–1040 Wien, Austria.

## Abstract

A  $k$ -*nucleus* of a normal rational curve in  $\text{PG}(n, F)$  is the intersection over all  $k$ -dimensional osculating subspaces of the curve ( $k \in \{-1, 0, \dots, n-1\}$ ). It is well known that for characteristic zero all nuclei are empty. In case of characteristic  $p > 0$  and  $\#F \geq n$  the number of non-zero digits in the representation of  $n+1$  in base  $p$  equals the number of distinct nuclei. An explicit formula for the dimensions of  $k$ -nuclei is given for  $\#F \geq k+1$ .

## 1 Introduction

Non-zero characteristic of the (commutative) ground field  $F$  heavily influences the geometric properties of Veronese varieties and, in particular, normal rational curves. Best known is probably the fact that in case of characteristic two all tangents of a conic are concurrent. This has lead to the concept of a *nucleus*. However, it seems that there are essentially distinct definitions. Some authors use the term “nucleus” to denote a point which completes a normal rational curve to a maximal arc ( $F$  a finite field of even order), others use the same term for the intersection of all osculating hyperplanes of a Veronese variety.

In the present paper we restrict ourselves to the discussion of normal rational curves in  $n$ -dimensional projective spaces over  $F$ . It turns out that in the ambient space of a normal rational curve there is a family of distinguished subspaces which will be called  $k$ -*nuclei*. Their definition is natural: A  $k$ -nucleus is the intersection over all  $k$ -dimensional osculating subspaces of the curve. The two types of nuclei mentioned above are just particular examples fitting into this general concept.

Our major result is a formula expressing the dimension of the  $k$ -nucleus of a normal rational curve in  $n$ -dimensional projective space for characteristic  $p > 0$ . For  $k = n - 1$  such a formula has been established by H. TIMMERMANN [16, 4.15]; cf. also [15]. Other results on nuclei are due to H. BRAUNER [1, 10.4.10], D.G. GLYNN [3, 49–50], A. HERZER [8], H. KARZEL [12], J.A. THAS [14], and J.A. THAS – J.W.P. HIRSCHFELD [11, 25.1].

---

\*Research supported by the Austrian National Science Fund (FWF), project P–12353–MAT.

It turns out that the geometric properties of a  $k$ -nucleus are closely related to binomial coefficients that vanish modulo  $p$  and, on the other hand, to the representations of the integers  $n$ ,  $n + 1$ , and  $k$  in base  $p$ . The zero entries of Pascal's triangle modulo  $p$  fall into various classes. The corresponding partition gives rise to three functions  $(T, \Phi, \Sigma)$  which form the backbone of our considerations. All this is discussed in Section 2 and then applied to geometry in Section 3.

Throughout this paper it will be assumed that the ground field has sufficiently many elements. Otherwise, our results on nuclei would become even more complicated, because one has to take into account that the elements of  $F$  are satisfying non-trivial polynomial identities.

## 2 On Pascal's Triangle modulo $p$

Throughout this section  $p$  denotes some fixed prime.

The representation of a non-negative integer  $n \in \mathbb{N} := \{0, 1, 2, \dots\}$  in base  $p$  has the form

$$n = \sum_{\lambda=0}^{\infty} n_{\lambda} p^{\lambda} =: \langle n_{\lambda} \rangle$$

with only finitely many digits  $n_{\lambda} \in \{0, 1, \dots, p-1\}$  different from 0. The following is well-known; cf., among others, [2, 364]:

**LEMMA 1 (Lucas)** *Let  $\langle n_{\lambda} \rangle$  and  $\langle j_{\lambda} \rangle$  be the representations of non-negative integers  $n$  and  $j$  in base  $p$ . Then*

$$\binom{n}{j} \equiv \prod_{\lambda=0}^{\infty} \binom{n_{\lambda}}{j_{\lambda}} \pmod{p}.$$

Since we are mainly interested in binomial coefficients that vanish modulo  $p$ , we adopt the following definition:

**DEFINITION 1** Given a prime  $p$  then define a half order on  $\mathbb{N}$  as follows:

$$\langle j_{\lambda} \rangle \preceq \langle n_{\lambda} \rangle \quad :\Leftrightarrow \quad j_{\lambda} \leq n_{\lambda} \text{ for all } \lambda \in \mathbb{N}.$$

Thus we have

$$\binom{n}{j} \equiv 0 \pmod{p} \quad \Longleftrightarrow \quad j \not\preceq n.$$

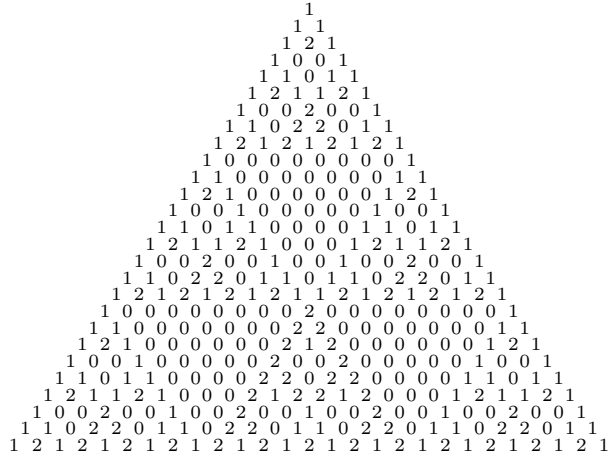
In the sequel the (infinite) Pascal triangle modulo  $p$  will be denoted by  $\Delta$ . In addition, we introduce an (infinite) *Pascal square* modulo  $p$  written as  $\square$ . Its  $(n, j)$ -entry is given by  $\binom{n}{j}$  modulo  $p$ , where  $n$  and  $j$  are non-negative integers. So the numbering of rows and columns will always start with the index 0. Clearly,  $\square$  is an infinite lower triangular matrix

$$\square = \Delta \nabla,$$

where each entry of  $\nabla$  is zero.

Moreover, let  $\square^i$  be the submatrix of  $\square$  that is formed by the rows and columns  $0, 1, \dots, p^i - 1$  with  $i \in \mathbb{N}$ . All entries of  $\square^i$  that are above the main

For example, let  $p = 3$  and consider the triangle  $\Delta^3$ :


$$\begin{array}{ccccccc}
& & & & \binom{0}{0} \Delta^i & & \\
& & & & \binom{1}{0} \Delta^i & \nabla^i & \binom{1}{1} \Delta^i \\
& & & \binom{2}{0} \Delta^i & \nabla^i & \binom{2}{1} \Delta^i & \nabla^i & \binom{2}{2} \Delta^i \\
& \cdots & & & & & & \\
\binom{p-1}{0} \Delta^i & \nabla^i & & \cdots & & & \nabla^i & \binom{p-1}{p-1} \Delta^i
\end{array}$$

Thus we get a partition of the zero entries of Pascal's triangle modulo  $p$  into maximal subtriangles  $\nabla^i$  ( $i \in \mathbb{N}^+$ ). If we add the infinite triangle  $\nabla$ , then a partition of the zero entries of Pascal's square modulo  $p$  is obtained. We get a coarser partition, by gluing together all triangles  $\nabla^i$  of same size to one class. A formal definition of this partition is as follows:

If we are given a fixed  $n \in \mathbb{N}$ , then  $\overline{i(n)}$  denotes the set of all elements  $j \in \mathbb{N}$  with  $(n, j) \in \overline{i}$ .

In the definition above the maximum  $L$  exists, since  $j \not\geq n$ . The infimum  $i$  is well-defined by the usual convention  $\inf \emptyset := \infty$ . It is easily seen that for each  $i \in \mathbb{N}^+ \cup \{\infty\}$  the set  $\bar{i}$  is non-empty, whence we actually have a partition.

A pair  $(n, j)$  is in  $\bar{i}$  if, and only if,  $j > n$ . The conditions, in terms of digits, for  $(n, j)$  to be in  $\bar{i} \neq \bar{\infty}$  are as follows:

$$\left. \begin{array}{ll} j_\lambda & \leq p-1 \quad \text{for all } \lambda \in \{0, 1, \dots, L-1\} \\ j_L & > n_L \quad \text{for one } L \in \{0, 1, \dots, i-1\} \\ j_\lambda & = n_\lambda \quad \text{for all } \lambda \in \{L+1, L+2, \dots, i-1\} \\ j_i & < n_i \\ j_\lambda & \leq n_\lambda \quad \text{for all } \lambda \in \{i+1, i+2, \dots\} \end{array} \right\} \quad (1)$$

In fact, the first line of (1) could be omitted. It simply says that there is no restriction on the digits  $j_0, j_1, \dots, j_{L-1}$ .

The essential properties of the classes  $\bar{i}$  and the sets  $\bar{i}(n)$  are described in the following Lemmas. We start with a “horizontal” result by counting the number of elements of class  $\bar{i} \neq \bar{\infty}$  belonging to a fixed row  $n$  of Pascal’s square modulo  $p$ .

**LEMMA 2** *Given  $n = \langle n_\lambda \rangle \in \mathbb{N}$  and  $i \in \mathbb{N}^+$  then*

$$\Phi(i, n) := \#\bar{i}(n) = (p^i - 1 - \sum_{\mu=0}^{i-1} n_\mu p^\mu) \cdot n_i \cdot \prod_{\lambda=i+1}^{\infty} (n_\lambda + 1). \quad (2)$$

*Proof.* We just have to count how the digits of  $j = \langle j_\lambda \rangle$  can be chosen so that (1) holds true. If we fix one  $L < i$ , then there are

$$p^L \cdot (p - 1 - n_L) \cdot 1^{i-L-1} \cdot n_i \cdot \prod_{\lambda=i+1}^{\infty} (n_\lambda + 1)$$

possibilities for  $j$ ; the factors in the formula above are corresponding to  $(j_0, j_1, \dots, j_{L-1})$ ,  $j_L$ ,  $(j_{L+1}, j_{L+2}, \dots, j_{i-1})$ ,  $j_i$ , and the remaining digits  $j_\lambda$ , respectively. Summing up gives then

$$\begin{aligned} \Phi(i, n) &= \left( \sum_{L=0}^{i-1} p^L (p - 1 - n_L) \right) \cdot n_i \cdot \prod_{\lambda=i+1}^{\infty} (n_\lambda + 1) \\ &= (p^i - 1 - \sum_{L=0}^{i-1} n_L p^L) \cdot n_i \cdot \prod_{\lambda=i+1}^{\infty} (n_\lambda + 1), \end{aligned}$$

as required. □

Note that  $\Phi(i, n)$  remains undefined for  $i = 0$  and  $i = \infty$ .

As an immediate consequence of Lemma 2 we obtain that

$$\Phi(i, n) = 0 \iff n_i = 0 \text{ or } n_{i-1} = \dots = n_1 = n_0 = p - 1, \quad (3)$$

where  $i \in \mathbb{N}^+$ . This result may be reformulated as follows:

**LEMMA 3** Let  $n = \langle n_\lambda \rangle \in \mathbb{N}$ ,  $i \in \mathbb{N}^+$ , and put

$$n + 1 =: b = \langle b_\lambda \rangle, \quad M := \min\{\lambda \mid b_\lambda \neq 0\}. \quad (4)$$

Then

$$\Phi(i, n) = \#\overline{i(n)} = 0 \iff \begin{cases} b_{i-1} &= 0 \text{ if } i \in \{1, 2, \dots, M\}, \\ b_i &= 0 \text{ if } i \in \{M+1, M+2, \dots\}. \end{cases} \quad (5)$$

*Proof.* We infer from the definition of  $M$  that

$$b = \langle \dots, b_{M+1}, b_M, 0, \dots, 0 \rangle \text{ and } n = \langle \dots, n_{M+1}, n_M, p-1, \dots, p-1 \rangle.$$

Therefore,  $b_M = n_M + 1$ ,  $0 \leq n_M < p-1$ , and

$$b_\lambda = n_\lambda \text{ for all } \lambda \in \{M+1, M+2, \dots\}. \quad (6)$$

So, by (3), the assertion holds true.  $\square$

The major advantage of formula (5) is that one has only to look at the non-zero digit  $b_M$  and the zero-digits of  $b$  in order to decide whether a set  $\overline{i(n)}$  is empty or not.

Next we investigate a “vertical” property of a class  $\bar{i} \neq \overline{\infty}$ :

**LEMMA 4** Let  $n \in \mathbb{N}$ ,  $i \in \mathbb{N}^+$ ,  $j \in \overline{i(n)}$ , and put

$$T := n - \sum_{\lambda=0}^{i-1} n_\lambda p^\lambda. \quad (7)$$

Then  $j \preceq T-1$  and  $j \in \overline{i(x)}$  for all  $x \in \{T, T+1, \dots, n\}$ .

*Proof.* We adopt the notations of (1). If  $x$  runs from  $n$  down to

$$n - \sum_{\lambda=0}^L n_\lambda p^\lambda = \langle \dots, n_{i+1}, n_i, \dots, n_{L+1}, 0, \dots, 0 \rangle, \quad (8)$$

then clearly  $j \in \overline{i(x)}$  by (1).

If  $n_{i-1} = \dots = n_{L+2} = n_{L+1} = 0$ , then we are finished, as

$$T-1 = n-1 - \sum_{\lambda=0}^L n_\lambda p^\lambda = \langle \dots, n_{i+1}, n_i-1, p-1, \dots, p-1 \rangle$$

and  $j \preceq T-1$ .

Otherwise, put  $L' := \min\{\lambda \in \{L+1, L+2, \dots, i-1\} \mid n_\lambda \neq 0\}$ . Subtracting 1 from both sides of (8) gives

$$n' := n-1 - \sum_{\lambda=0}^L n_\lambda p^\lambda = \langle \dots, n_{i+1}, n_i, \dots, n_{L'}-1, p-1, \dots, p-1 \rangle.$$

By  $j_{L'} = n_{L'}$ , we obtain  $j_{L'} > n_{L'}-1$ , whence  $j \in \overline{i(n')}$ . If  $T'$  is defined according to (7) by replacing  $n$  with  $n'$ , then  $T' = T$ .

So, if we proceed with  $n'$  and  $j$  as above, then the required result follows after a finite number of steps.  $\square$

With the settings of the previous Lemma put  $T =: \langle T_\lambda \rangle$ . Then  $j \in \overline{i(T)}$  implies  $j_i < T_i = n_i$  and  $j_\lambda \leq T_\lambda = n_\lambda$  for all  $\lambda \in \{i+1, i+2, \dots\}$ . Hence

$$Y := j - \sum_{\lambda=0}^{i-1} j_\lambda p^\lambda = \langle \dots, j_{i+1}, j_i, 0, \dots, 0 \rangle \preceq T$$

and

$$Y + p^i = \langle \dots, j_{i+1}, j_i + 1, 0, \dots, 0 \rangle \preceq T,$$

whereas  $\{Y + 1, Y + 2, \dots, Y + p^i - 1\} \subset \overline{i(T)}$ . By the well known recurrence  $\binom{r}{s} + \binom{r}{s+1} = \binom{r+1}{s+1}$ , it follows that line  $T$  of Pascal's triangle modulo  $p$  is the top line of a subtriangle  $\nabla^i$  which is surrounded by non-zero entries. Observe that the number  $T$  does not depend on the choice of  $j \in \overline{i(n)}$ .

From here the following is easily seen: Given an  $i \in \mathbb{N}^+$  and  $n, j \in \mathbb{N}$  then  $(n, j) \in \overline{i}$  if, and only if, the  $(n, j)$ -entry of Pascal's square modulo  $p$  is in one maximal subtriangle  $\nabla^i$ . The class  $\overline{\infty}$  corresponds to the infinite triangle  $\nabla$  of Pascal's square modulo  $p$ .

Obviously, the definition of  $T$  in (7) still makes sense if  $n, i \in \mathbb{N}$  are arbitrary. However, as in Lemma 3, we change from  $n$  to  $n + 1 =: b$ , as we prefer to use (5) rather than (3) when characterizing non-empty sets  $\overline{i(n)}$ . So we put

$$T(R, b) := b - \sum_{\lambda=0}^{R-1} b_\lambda p^\lambda \text{ for all } R \in \mathbb{N} \cup \{\infty\}. \quad (9)$$

We read off from (4) and (5) that the "top line function"  $T(R, b)$  satisfies

$$0 = T(\infty, b) \leq \dots \leq T(M+2, b) \leq T(M+1, b) < T(M, b) = \dots = T(0, b) = b. \quad (10)$$

In fact, if  $R \in \mathbb{N}$  is chosen sufficiently large, then  $T(R, b) = 0$ .

For each non-empty set  $\overline{i(n)} \neq \overline{\infty}$  it follows from (5) that  $i > M$ . So, by (6), the number  $T(i, b)$  coincides with the corresponding bound (7). Moreover, we have

$$T(i, b) - 1 = \langle \dots, n_{i+1}, n_i - 1, p - 1, \dots, p - 1 \rangle = \max \overline{i(n)}, \quad (11)$$

since  $\overline{i(n)} \neq \emptyset$  implies that at least one of the digits  $n_0, n_1, \dots, n_{i-1}$  is smaller than  $p - 1$  and  $b_i = n_i > 0$ . Finally, by (5),

$$\overline{i_1(n)} \neq \emptyset \neq \overline{i_2(n)} \text{ and } i_1 > i_2 \text{ implies } T(i_1, b) < T(i_2, b). \quad (12)$$

If  $i \in \{1, 2, \dots, M\}$ , then  $\overline{i(n)} = \emptyset$  and  $T(i, b) = b > n$  expresses the fact that line  $n$  of Pascal's triangle modulo  $p$  does not meet a subtriangle  $\nabla^i$ . For  $i \in \{M+1, M+2, \dots\}$  with  $\overline{i(n)} = \emptyset$ , formula (5) implies  $T(i, b) = T(i+1, b)$ .

The following result gives the essential information on zero-entries in line  $n$  of Pascal's triangle modulo  $p$ :

**LEMMA 5** *Let  $n \in \mathbb{N}$  and  $i \in \mathbb{N}^+$ . Then*

$$\begin{aligned}
\Sigma(i, n) &:= \sum_{\eta=i}^{\infty} \Phi(\eta, n) \\
&= \#(\overline{i(n)} \cup \overline{(i+1)(n)} \cup \dots) \\
&= n+1 - \left(1 + \sum_{\mu=0}^{i-1} n_{\mu} p^{\mu}\right) \prod_{\lambda=i}^{\infty} (n_{\lambda} + 1).
\end{aligned} \tag{13}$$

*Proof.* (a) We are going to determine all integers  $j = \langle j_{\lambda} \rangle$  such that  $j \preceq n$ . Clearly, each digit  $j_{\lambda}$  can be chosen in exactly  $n_{\lambda} + 1$  ways to meet this condition. Hence there are

$$\prod_{\lambda=0}^{\infty} (n_{\lambda} + 1) = n + 1 - \Sigma(1, n) \tag{14}$$

such elements and (13) holds true for  $i = 1$ . In fact, (14) is well known; cf., e.g., [9, 98].

(b) Suppose that (13) has been established for  $i \geq 1$ . We infer from (2) and (13) that

$$\begin{aligned}
\Sigma(i+1, n) &= \Sigma(i, n) - \Phi(i, n) \\
&= n+1 - \left(1 + \sum_{\xi=0}^{i-1} n_{\xi} p^{\xi}\right) \prod_{\nu=i}^{\infty} (n_{\nu} + 1) \\
&\quad - (p^i - 1 - \sum_{\mu=0}^{i-1} n_{\mu} p^{\mu}) n_i \prod_{\lambda=i+1}^{\infty} (n_{\lambda} + 1) \\
&= n+1 - \left(1 + \sum_{\xi=0}^i n_{\xi} p^{\xi}\right) \prod_{\nu=i+1}^{\infty} (n_{\nu} + 1)
\end{aligned}$$

which completes the proof.  $\square$

Formula (13) has the nice property that with increasing  $i$  one digit after another moves from the product on the right to the sum on the left where it is then multiplied with the corresponding power of  $p$ .

### 3 Nuclei

Let  $\text{PG}(n, F)$  be the  $n$ -dimensional projective space on  $F^{n+1}$ , where  $n \geq 2$  and  $F$  is a (commutative) field.

Each *normal rational curve* (NRC) is projectively equivalent to the NRC

$$\Gamma := \{F(1, t, \dots, t^n) \mid t \in F \cup \{\infty\}\}. \tag{15}$$

Note that  $t = \infty$  yields the point  $F(0, \dots, 0, 1)$ . The subsequent exposition follows [5] and uses the non-iterative derivation of polynomials due to H. HASSE, F.K. SCHMIDT, and O. TEICHMÜLLER; cf., e.g., [4] or [10, 1.3].

The column vectors of the matrix

$$C_t := \begin{pmatrix} \binom{0}{0} & 0 & 0 & \dots & 0 \\ \binom{1}{0}t & \binom{1}{1} & 0 & \dots & 0 \\ \binom{2}{0}t^2 & \binom{2}{1}t & \binom{2}{2} & \dots & 0 \\ \vdots & & & \ddots & \vdots \\ \binom{n}{0}t^n & \binom{n}{1}t^{n-1} & \binom{n}{2}t^{n-2} & \dots & \binom{n}{n} \end{pmatrix} \quad (16)$$

with  $t \in F$  are (from the left to the right) written as  $c_t, c'_t, \dots, c_t^{(n-1)}, c_t^{(n)}$  and yield the *derivative points* of the parametric representation (15). Moreover, we put  $c_\infty^{(k)} := (\delta_{0,n-k}, \dots, \delta_{n,n-k})$ . The *osculating  $k$ -subspace* ( $k \in \{-1, 0, \dots, n-1\}$ ) of  $\Gamma$  at the point  $Fc_t$  is

$$\text{span} \{Fc_t, Fc'_t, \dots, Fc_t^{(k)}\} =: \mathcal{S}_t^{(k)}\Gamma.$$

All osculating subspaces at  $Fc_t$  form a chain with  $\dim \mathcal{S}_t^{(k)}\Gamma = k$ .

We infer from  $C_t^{-1} = C_{-t}$  that the osculating subspace  $\mathcal{S}_t^{(k)}\Gamma$  ( $t \in F$ ) equals the set of all points  $F(x_0, \dots, x_n)$  satisfying the following linear system:

$$\left. \begin{array}{rcl} \binom{k+1}{0}(-t)^{k+1}x_0 + \binom{k+1}{1}(-t)^k x_1 + \dots + \binom{k+1}{k+1}x_{k+1} & = & 0 \\ \binom{k+2}{0}(-t)^{k+2}x_0 + \binom{k+2}{1}(-t)^{k+1}x_1 + \dots + \binom{k+2}{k+2}x_{k+2} & = & 0 \\ \vdots & & \vdots \\ \binom{n}{0}(-t)^n x_0 + \binom{n}{1}(-t)^{n-1}x_1 + \dots + \binom{n}{n}x_n & = & 0 \end{array} \right\} \quad (17)$$

On the other hand,  $\mathcal{S}_\infty^{(k)}\Gamma$  is given by the linear system

$$x_0 = x_1 = \dots = x_{n-k-1} = 0. \quad (18)$$

**REMARK 1** Each semilinear bijection  $\tau \in \Gamma L(2, F)$  acts on the NRC (15) in a well-known way: A point  $Fc_t$  with  $t = t_1 t_0^{-1}$ ,  $(t_0, t_1) \in F^2 \setminus \{(0, 0)\}$  goes over to  $Fc_{\tilde{t}}$ , where  $\tilde{t} := \tilde{t}_1 \tilde{t}_0^{-1}$  and  $(\tilde{t}_0, \tilde{t}_1) := \tau(t_0, t_1)$ . This bijection of  $\Gamma$  extends to an automorphic collineation of  $\Gamma$  that preserves all osculating subspaces. Thus a collineation group  $G^{(n-1)}$  isomorphic to  $\text{P}\Gamma L(2, F)$  is obtained.

In fact, the NRC (15) gives rise to a family  $G^{(k)}$  ( $k \in \{0, 1, \dots, n-1\}$ ) of collineation groups of  $\text{PG}(n, F)$  as follows:  $G^{(k)}$  is defined by the property that the system of all osculating  $r$ -subspaces with  $r \leq k$  remains invariant.

Hence  $G^{(0)}$  is the group of all collineations fixing  $\Gamma$ , as a set of points. If  $\#F \geq n+2$  or  $n=2$ , then  $G^{(0)} = G^{(n-1)}$ . Otherwise, there are automorphic collineations of the NRC that do not preserve all osculating subspaces, whence the concept of osculating subspaces depends on the parametric representation of the NRC rather than on the points of the NRC [6], [7, 2.4].

Instead of a parametric representation one could also use a *generating map* in order to define osculating subspaces. This point of view has been adopted in [5] and [7]. Cf. also [8] for further remarks on the phenomena arising for a “small” ground field.



In all results of the present paper a NRC  $\Gamma$  is understood as a set of points endowed with a fixed parametric representation which arises from (15) by applying a projective collineation.

**DEFINITION 3** The  $k$ -nucleus  $\mathcal{N}^{(k)}\Gamma$  ( $k \in \{-1, 0, \dots, n-1\}$ ) of a normal rational curve  $\Gamma$  in  $\text{PG}(n, F)$  is the intersection over all its osculating  $k$ -subspaces.

The nuclei of a NRC  $\Gamma$  yield an ascending chain

$$\emptyset = \mathcal{N}^{(-1)}\Gamma = \mathcal{N}^{(0)}\Gamma = \dots = \mathcal{N}^{(r)}\Gamma \subset \dots \subset \mathcal{N}^{(n-1)}\Gamma \quad (r := \lfloor \frac{n-1}{2} \rfloor), \quad (19)$$

because  $\mathcal{S}_0^k\Gamma \cap \mathcal{S}_\infty^k\Gamma = \emptyset = \mathcal{N}^{(k)}\Gamma$  for all  $k \in \{-1, 0, \dots, r\}$ .

In the following result nuclei of a NRC are linked with binomial coefficients that vanish modulo the characteristic of  $F$ .

**THEOREM 1** *If  $F$  has at least  $k+1$  elements, then the nucleus  $\mathcal{N}^{(k)}\Gamma$  of the normal rational curve (15) equals the subspace  $\mathcal{Q}$  spanned by those base points  $P_j$  of the standard frame of reference, where  $j \in \{0, 1, \dots, n\}$  is subject to*

$$\binom{k+1}{j} \equiv \binom{k+2}{j} \equiv \dots \equiv \binom{n}{j} \equiv 0 \pmod{\text{char } F}. \quad (20)$$

*Proof.* (a) Let  $F(x_0, x_1, \dots, x_n)$  be a point of  $\mathcal{N}^{(k)}\Gamma$ . By (18) and  $\#F \geq k+1$ , every left hand side term in (17) is a zero-polynomial in  $t$ . Hence  $x_j \neq 0$  implies (20), whence the point belongs to  $\mathcal{Q}$ .

(b) Suppose that (20) holds true for some  $j$ . As  $\binom{r-1}{s} \equiv \binom{r}{s} \equiv 0 \pmod{\text{char } F}$  implies  $\binom{r-1}{s-1} \equiv 0 \pmod{\text{char } F}$ , it follows that

$$\binom{k+1}{j-l} \equiv \binom{k+2}{j-l} \equiv \dots \equiv \binom{n-l}{j-l} \equiv 0 \pmod{\text{char } F}$$

for all  $l \in \{0, 1, \dots, n-k-1\}$ . So  $j > n-k-1$ .

(c) Let  $F(x_0, x_1, \dots, x_n)$  be a point in  $\mathcal{Q}$ . By (b),  $x_0 = x_1 = \dots = x_{n-k-1} = 0$  in accordance with (18). If  $x_j \neq 0$ , then (20) shows that  $(x_0, x_1, \dots, x_n)$  is also a solution of (17) for all  $t \in F$ . So the point lies in  $\mathcal{N}^{(k)}\Gamma$ .  $\square$

By Theorem 1,  $\text{char } F = 0$  implies  $\mathcal{N}^{(n-1)}\Gamma = \emptyset$ , whence here the nuclei of a NRC cannot deserve interest. Thus we assume in the remaining part of this section that

$$\begin{aligned} \text{char } F &=: p > 0, \\ n &=: \langle n_\lambda \rangle \quad (\text{in base } p), \\ n+1 &=: b =: \langle b_\lambda \rangle \quad (\text{in base } p). \end{aligned}$$

We shall frequently use the “top line function”  $T(R, b)$  together with the “cardinality functions”  $\Phi(i, n)$  and  $\Sigma(i, n)$  that have been defined in Section 2.

**THEOREM 2** *Let  $\Gamma$  be a normal rational curve in  $\text{PG}(n, F)$ . If  $k$  is an integer satisfying  $\#F \geq k+1$  and*

$$T(R, b) = b - \sum_{\mu=0}^{R-1} b_\mu p^\mu \leq k+1 < b - \sum_{\lambda=0}^{Q-1} b_\lambda p^\lambda = T(Q, b) \quad (21)$$

with at most one  $b_\lambda \neq 0$  for  $\lambda \in \{Q, Q+1, \dots, R-1\}$ , then the  $k$ -nucleus of  $\Gamma$  has dimension

$$\dim \mathcal{N}^{(k)} \Gamma = n - \left(1 + \sum_{\mu=0}^{R-1} n_\mu p^\mu\right) \prod_{\lambda=R}^{\infty} (n_\lambda + 1) = \Sigma(R, n) - 1. \quad (22)$$

*Proof.* There is exactly one  $N \in \{Q, Q+1, \dots, R-1\}$  with  $b_N \neq 0$ , because of the strict inequality in (21). Consequently,

$$T(R, b) = T(R-1, b) = \dots = T(N+1, b) < T(N, b) = \dots = T(Q, b). \quad (23)$$

By Theorem 1,  $\dim \mathcal{N}^{(k)} \Gamma + 1$  is equal to the number of elements  $j \in \{0, 1, \dots, n\}$  with property (20). If we are given an integer  $i \geq 1$ , then the conditions

$$\overline{i(n)} \neq \emptyset \text{ and } T(i, b) \leq k+1 \quad (24)$$

together are equivalent to the existence of an element  $j \in \overline{i(n)}$  satisfying (20). By Lemma 4, if (20) holds for at least one  $j \in \overline{i(n)}$ , then it is true for all elements of  $\overline{i(n)}$ . There are three possibilities:

For  $1 \leq i \leq N$  we read off from (10), (23), and (21) that  $k+1 < T(Q, b) = T(N, b) \leq T(i, b)$  which contradicts (24).

For  $N+1 \leq i \leq R-1$  we obtain  $\overline{i(n)} = \emptyset$  by virtue of (5). Hence (24) does not hold true.

Given an  $i \geq R$  then  $T(i, b) \leq T(R, b) \leq k+1$  by (10) and (21). So the class  $\overline{i}$  yields exactly  $\Phi(i, n) \geq 0$  distinct solutions of (20).

Thus the number of elements  $j$  which satisfy (20) is given by

$$\sum_{i=R}^{\infty} \Phi(i, n) = \Sigma(R, n).$$

This completes the proof.  $\square$

Next we establish an easy formula for the number of distinct nuclei:

**THEOREM 3** *Let  $\Gamma$  be a normal rational curve in  $\text{PG}(n, F)$  and assume that  $F$  has at least  $n$  elements. Then the number  $d$  of non-zero digits in the representation of  $b = n+1$  in base  $p$  is equal to the number of distinct nuclei of  $\Gamma$ .*

*Proof.* Let  $N_1 < N_2 < \dots < N_d$  be the positions of the non-zero digits of  $b$  in base  $p$ . From (10) and (12),  $0 = T(N_d+1, b) < T(N_d, b)$ ,

$$T(N_{\alpha+1}, b) = T(N_\alpha+1, b) < T(N_\alpha, b) \text{ for all } \alpha \in \{d-1, d-2, \dots, 1\},$$

and  $T(N_1, b) = b$ . Thus we obtain  $d$  distinct “consecutive” inequalities

$$T(N_\alpha+1, b) \leq k+1 < T(N_\alpha, b) \quad (\alpha \in \{d, d-1, \dots, 1\}). \quad (25)$$

So each  $k \in \{-1, 0, \dots, n-1\}$  is a solution of one and only one inequality (25). It is immediate from (5) and (13) that

$$0 = \Sigma(N_d+1, n) < \Sigma(N_{d-1}+1, n) < \dots < \Sigma(N_1+1, n),$$

whence distinct inequalities (25) correspond to distinct dimensions of nuclei.  $\square$

There is always at least one inequality (25). Put

$$J := N_d = \max\{\lambda \mid b_\lambda \neq 0\}.$$

It follows from (25), with  $\alpha := d$ , and (22) that

$$\mathcal{N}^{(k)}\Gamma = \emptyset \text{ for all } k \in \{-1, 0, \dots, b_J p^J - 2\} \quad (\#F \geq k + 1). \quad (26)$$

This improves the bound given in formula (19).

The number  $k := n - 1$  is a solution of the inequality (25) obtained for  $\alpha := 1$ . As before, let

$$M := N_1 = \min\{\lambda \mid b_\lambda \neq 0\}.$$

By (5),  $\Sigma(1, n) = \Sigma(2, n) = \dots = \Sigma(M + 1, n)$ . Now (14) implies that (22) can be rewritten as

$$\dim \mathcal{N}^{(n-1)}\Gamma = n - \prod_{\lambda=0}^{\infty} (n_\lambda + 1) \quad (\#F \geq n). \quad (27)$$

Cf. [16, 4.15].

**REMARK 2** The following example illustrates Theorems 2 and 3: Let  $p = 3$ ,  $n = 305 = \langle 1, 0, 2, 0, 2, 2 \rangle$ , and assume that the ground field  $F$  has at least  $n$  elements. Then  $b = 306 = \langle 1, 0, 2, 1, 0, 0 \rangle$  and we get the following table for  $\dim \mathcal{N}^{(k)}\Gamma$ :

$$\begin{aligned} \langle 0, 0, 0, 0, 0, 0 \rangle = 0 \leq k + 1 < 243 = \langle 1, 0, 0, 0, 0, 0 \rangle &\implies \dim \mathcal{N}^{(k)}\Gamma = -1 \\ \langle 1, 0, 0, 0, 0, 0 \rangle = 243 \leq k + 1 < 297 = \langle 1, 0, 2, 0, 0, 0 \rangle &\implies \dim \mathcal{N}^{(k)}\Gamma = 179 \\ \langle 1, 0, 2, 0, 0, 0 \rangle = 297 \leq k + 1 < 306 = \langle 1, 0, 2, 1, 0, 0 \rangle &\implies \dim \mathcal{N}^{(k)}\Gamma = 251 \end{aligned}$$

**REMARK 3** The NRC  $\Gamma$  admits a group  $G^{(n-1)}$  of collineations preserving all osculating subspaces; see Remark 1. The group  $G^{(n-1)}$  acts 3-fold transitively on  $\Gamma$ . All nuclei and the entire space are  $G^{(n-1)}$ -invariant subspaces. However, there may be other  $G^{(n-1)}$ -invariant subspaces:

Suppose that  $p = 2$ ,  $n = 4$ , and  $\#F \geq 4$ . By (16), we have

$$C_t = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ t & 1 & 0 & 0 & 0 \\ t^2 & 0 & 1 & 0 & 0 \\ t^3 & t^2 & t & 1 & 0 \\ t^4 & 0 & 0 & 0 & 1 \end{pmatrix}$$

with  $t \in F$ . The bottom line of the matrix shows that  $\dim \mathcal{N}^{(3)}\Gamma = 2$ , whereas all other nuclei are empty. Obviously, all derivative points  $Fc'_t$  ( $t \in F \cup \{\infty\}$ ) are on the line joining the base points  $P_1$  and  $P_3$ . There is a unique transversal line for three skew lines spanning  $\text{PG}(4, F)$ . The tangents of  $\Gamma$  at  $Fc_0$ ,  $Fc_1$ , and  $Fc_\infty$  are mutually skew and spanning the entire space. Hence there is no line other than  $P_1P_3$  that is meeting all tangents of  $\Gamma$ . Therefore, the line  $P_1P_3 \subset \mathcal{N}^{(3)}\Gamma$  is  $G^{(n-1)}$ -invariant.

**REMARK 4** Let  $R > Q \geq 0$  be integers with

$$b_R \neq 0 = b_{R-1} = \dots = b_{Q+1} \neq b_Q$$

and put

$$k := T(R, b) - 1 = \langle \dots, n_{R+1}, n_R - 1, p - 1, \dots, p - 1 \rangle.$$

So  $k$  is a *minimal* solution of the inequality (21). By assuming  $\#F \geq k + 1$ , Theorem 2 shows that  $\mathcal{N}^{(k)}\Gamma$  is a non-empty nucleus. We aim at characterizing the osculating  $k$ -subspaces of  $\Gamma$  among the  $k$ -dimensional subspaces passing through  $\mathcal{N}^{(k)}\Gamma$ .

Theorem 1 describes a basis of  $\mathcal{N}^{(k)}\Gamma$ . By (11) and (12), the greatest index  $j$  of a base point  $P_j$  appearing in that basis is  $T(R, b) - 1 = k$ , whence  $k \in \overline{R(n)}$ . We define

$$U := \max\{j \in \mathbb{N} \mid j < k \text{ and } j \preceq n\} = \langle \dots, n_{R+1}, n_R - 1, n_{R-1}, \dots, n_0 \rangle.$$

The osculating  $U$ -subspace  $\mathcal{S}_0^{(U)}\Gamma$  at  $P_0$  is spanned by the base points  $P_0, P_1, \dots, P_U$  so that

$$\mathcal{S}_0^{(U)}\Gamma \vee \mathcal{N}^{(k)}\Gamma = \mathcal{S}_0^{(k)}\Gamma.$$

Here the minimality of  $k$  is essential. By virtue of the collineation group  $G^{(n-1)}$ , this property carries over from  $P_0 = Fc_0$  to all points of  $\Gamma$ . Therefore, for our specific choice of  $k$ , the following holds true:

A  $k$ -dimensional subspace through  $\mathcal{N}^{(k)}\Gamma$  is an osculating subspace of  $\Gamma$  if, and only if, it contains an osculating  $U$ -subspace of  $\Gamma$ .

In particular, for  $n = p = 2$  and  $k = 1$  this is well known. Here  $U = 0$  and a characterization of the tangents of a conic  $\Gamma$  among the lines through the nucleus  $\mathcal{N}^{(1)}\Gamma$  is obtained. Cf. also [8, Satz 2].

**REMARK 5** Let  $\#F \geq k$ . If  $\mathcal{N}^{(k)}\Gamma$  consists of one point only, then necessarily  $\Phi(i, n) = 1$  for some  $i \in \mathbb{N}^+$ . Thus all factors in (2) are equal to 1 which is easily seen to be equivalent to

$$n = 2p^i - 2. \tag{28}$$

Conversely, (28) implies  $b = n + 1 < p^{i+1}$  so that  $\Sigma(i + 1, n) = 0$  by (5). Hence,  $\Phi(i, n) = \Sigma(i, n) = 1$ , as required. Thus (28) implies that there is a point off the NRC which is fixed by all collineations of the group  $G^{(n-1)}$ . This point is the base point  $P_{p^i-1}$ . Cf. also [14] and [3, 49–50].

## References

- [1] BRAUNER, H., *Geometrie projektiver Räume II*, BI-Wissenschaftsverlag, Mannheim Wien Zürich, 1976.
- [2] BROUWER, A.E., AND WILBRINK, H.A., *Block Designs*, in Handbook of Incidence Geometry, Buekenhout, F., ed., Elsevier, Amsterdam, 1995, ch. 8, pp. 349–382.

- [3] GLYNN, D.G., *The non-classical 10-arc of  $PG(4, 9)$* , Discrete Math., 59 (1986), pp. 43–51.
- [4] HASSE, H., *Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten*, J. reine angew. Math., 177 (1937), pp. 215–237.
- [5] HAVLICEK, H., *Normisomorphismen und Normkurven endlichdimensionaler projektiver Desargues-Räume*, Monatsh. Math., 95 (1983), pp. 203–218.
- [6] HAVLICEK, H., *Die automorphen Kollineationen nicht entarteter Normkurven*, Geom. Dedicata, 16 (1984), pp. 85–91.
- [7] HAVLICEK, H., *Applications of Results on Generalized Polynomial Identities in Desarguesian Projective Spaces*, in Rings and Geometry, Kaya, R., Plaumann, P., and Strambach, K., eds., D. Reidel, Dordrecht, 1985, pp. 39–77.
- [8] HERZER, A., *Die Schmieghyperebenen an die Veronese-Mannigfaltigkeit bei beliebiger Charakteristik*, J. Geometry, 18 (1982), pp. 140–154.
- [9] HEXEL, E., AND SACHS, H., *Counting residues modulo a prime in Pascal's triangle*, Indian J. Math., 20 (1978), pp. 91–105.
- [10] HIRSCHFELD, J.W.P., *Projective Geometry over Finite Fields*, Clarendon Press, Oxford, second ed., 1998.
- [11] HIRSCHFELD, J.W.P., AND THAS, J.A., *General Galois Geometries*, Oxford University Press, Oxford, 1991.
- [12] KARZEL, H., *Über einen Fundamentalsatz der synthetischen algebraischen Geometrie von W. Burau und H. Timmermann*, J. Geometry, 28 (1987), pp. 86–101.
- [13] LONG, C.T., *Pascal's triangle modulo  $p$* , Fibonacci Q., 19 (1981), pp. 458–463.
- [14] THAS, J.A., *Normal rational curves and  $(q + 2)$ -arcs in a Galois space  $S_{q-2, q}$  ( $q = 2^h$ )*, Atti Accad. Naz. Lincei Rend., 47 (1969), pp. 249–252.
- [15] TIMMERMAN, H., *Descrizioni geometriche sintetiche di geometrie proiettive con caratteristica  $p > 0$* , Ann. mat. pura appl., IV. Ser. 114, (1977), pp. 121–139.
- [16] TIMMERMAN, H., *Zur Geometrie der Veronesemannigfaltigkeit bei endlicher Charakteristik*, Habilitationsschrift, Univ. Hamburg, 1978.